PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282803

(43)Date of publication of application : 15.10.1999

(51)Int.CI. G06F 15/00

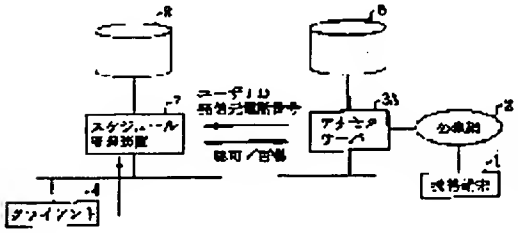
(21)Application number : 10-081789

(22)Date of filing : 27.03.1998

(71)Applicant : MITSUBISHI ELECTRIC CORP

(72)Inventor : ARAKI TOSHIO
SHIMIZU MICHIO
KATO ATSUSHI
SAITO TAKUMA
MATSUHIRA KEIICHI

(54) ILLEGAL ACCESS PREVENTION SYSTEM



(57)Abstract:

PROBLEM TO BE SOLVED: To double decide the propriety of connection and accordingly to improve the security.

SOLUTION: A schedule management device 7 receives a user ID and the telephone number of an originator from a server 3A, compares the received telephone number with the telephone number of the originator previously registered and informs the server 3A of the comparison result. Receiving the comparison result from the device 7, the server 3A notifies a portable terminal of the permission and rejection of access when coincidence and no coincidence are confirmed between both telephone numbers of the originator respectively.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

（書誌＋要約＋請求の範囲）

---

(19)【発行国】日本国特許庁（ＪＰ）
(12)【公報種別】公開特許公報（Ａ）
(11)【公開番号】特開平１１－２８２８０３
(43)【公開日】平成１１年（１９９９）１０月１５日
(54)【発明の名称】不正アクセス防止システム
(51)【国際特許分類第６版】
G06F 15/00 330
【ＦＩ】
G06F 15/00 330 B
【審査請求】未請求
【請求項の数】５
【出願形態】ＯＬ
【全頁数】１４
(21)【出願番号】特願平１０－８１７８９
(22)【出願日】平成１０年（１９９８）３月２７日
(71)【出願人】
【識別番号】０００００６０１３
【氏名又は名称】三菱電機株式会社
【住所又は居所】東京都千代田区丸の内二丁目２番３号
(72)【発明者】
【氏名】荒木 敏夫
【住所又は居所】東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)【発明者】
【氏名】清水 道夫
【住所又は居所】東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)【発明者】
【氏名】加藤 敦史
【住所又は居所】東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)【発明者】
【氏名】齋藤 琢磨
【住所又は居所】東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)【発明者】
【氏名】松比良 啓一
【住所又は居所】東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内

(74)【代理人】
【弁理士】
【氏名又は名称】曾我 道照 （外６名）

---

(57)【要約】
【課題】 従来の不正アクセス防止システムでは、パスワードが第三者に漏れる可能性があるという課題があった。
【解決手段】 アクセスサーバ３Ａからユーザ ＩＤ及び発信元電話番号を受け取り前記発信元電話番号と予め登録された発信元電話番号と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置７を備え、アクセスサーバ３Ａは、前記スケジュール管理装置から前記比較結果を受け取り前記発信元電話番号同士が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知する。
【効果】 ２重に接続可否を判定することになり、セキュリティの強化を図ることができる。

【特許請求の範囲】
【請求項１】 携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤ及び第１のユーザ識別情報を受け取り前記第１のユーザ識別情報とスケジュールテーブルに予め登録された第２のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤ及び第１のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第１及び第２のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知することを特徴とする不正アクセス防止システム。
【請求項２】 携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末

に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤを受け取り前記ユーザＩＤに基づきスケジュールテーブルから予め登録された第２のユーザ識別情報を読み出して前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第２のユーザ識別情報を受け取り前記第１及び第２のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知することを特徴とする不正アクセス防止システム。

【請求項３】 前記第１及び第２のユーザ識別情報は、前記携帯端末の発信元電話番号であることを特徴とする請求項１又は２記載の不正アクセス防止システム。

【請求項４】 前記第１のユーザ識別情報は、前記携帯端末の位置情報であり、前記第２のユーザ識別情報は、前記登録された位置情報であることを特徴とする請求項１又は２記載の不正アクセス防止システム。

【請求項５】 前記第１のユーザ識別情報は、前記携帯端末の発信元電話番号及び位置情報であり、前記第２のユーザ識別情報は、前記携帯端末の発信元電話番号及び前記登録された位置情報であることを特徴とする請求項１又は２記載の不正アクセス防止システム。

詳細な説明

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、企業などの組織内ネットワークへの公衆網を介したアクセスにおいて、第三者からの不正なアクセスを防止する不正アクセス防止システムに関するものである。

【０００２】

【従来の技術】従来の不正アクセス防止システムについて図面を参照しながら説明する。図１９は、従来の不正アクセス防止システムの構成を示す図である。

【０００３】図１９において、１は携帯端末、２は公衆網、３は組織内ネットワークのアクセスサーバ、４は組織内ネットワークのクライアント、５は組織内ネットワークのサーバである。

【０００４】携帯端末１から公衆網２経由で組織内ネットワークへ接続し、内部のコンピュータを利用する場合、組織内ネットワークへ接続する際に、正規のユーザからの接続要求であるか否かを判定し、セキュリティを確保する必要がある。このセキュリティ確保は、

組織内ネットワークのアクセスサーバ３でアクセスの制御を行うことにより達成されている。

【０００５】図１９に示すように、あらかじめ組織内ネットワークへのアクセスが許可されたユーザ毎に、「ユーザＩＤ」と、「パスワード」とを設定する。アクセスサーバ３は、アクセス開始時にユーザＩＤとパスワードをユーザに要求し、許可されているユーザＩＤとパスワードが一致したときに、組織内ネットワークへのアクセスを許可する。

【０００６】

【発明が解決しようとする課題】上述したような従来の不正アクセス防止システムでは、パスワードが第三者に漏れる可能性があり、それを悪用して組織内ネットワークへ接続される恐れがあるという問題点があった。

【０００７】この発明は、前述した問題点を解決するためになされたもので、組織外にある端末から公衆網経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置とアクセスサーバを連携させ、ユーザＩＤ、パスワード、発信電話機の番号、個人の行動に合わせた接続可否を判定することにより、セキュリティの強化を図ることができる不正アクセス防止システムを得ることを目的とする。

【０００８】

【課題を解決するための手段】この発明に係る不正アクセス防止システムは、携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤ及び第１のユーザ識別情報を受け取り前記第１のユーザ識別情報とスケジュールテーブルに予め登録された第２のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤ及び第１のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第１及び第２のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知するものである。

【０００９】この発明に係る不正アクセス防止システムは、携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤを受け取り前記ユーザＩＤに基づきスケジュールテーブルから予め登録された第２のユーザ識別情報を読み出して前記アクセスサーバ

に通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第２のユーザ識別情報を受け取り前記第１及び第２のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するものである。

【００１０】また、この発明に係る不正アクセス防止システムは、前記第１及び第２のユーザ識別情報を、前記携帯端末の発信元電話番号としたものである。

【００１１】また、この発明に係る不正アクセス防止システムは、前記第１のユーザ識別情報を、前記携帯端末の位置情報とし、前記第２のユーザ識別情報を、前記登録された位置情報としたものである。

【００１２】さらに、この発明に係る不正アクセス防止システムは、前記第１のユーザ識別情報を、前記携帯端末の発信元電話番号及び位置情報とし、前記第２のユーザ識別情報を、前記携帯端末の発信元電話番号及び前記登録された位置情報としたものである。

【００１３】

【発明の実施の形態】実施の形態１．この発明の実施の形態１に係る不正アクセス防止システムについて図面を参照しながら説明する。図１は、この発明の実施の形態１に係る不正アクセス防止システムの構成を示す図である。なお、各図中、同一符号は同一又は相当部分を示す。

【００１４】図１において、１は携帯端末、２は公衆網、３Ａは組織内ネットワークのアクセスサーバ、４は組織内ネットワークのクライアント、６はユーザ毎のユーザＩＤとパスワードが登録されているファイル装置、７は組織内ネットワークのスケジュール管理装置、８は個人のスケジュールテーブルが登録されているファイル装置である。

【００１５】図２は、この発明の実施の形態１に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【００１６】図２に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザー人について「ユーザ番号」と、「ユーザＩＤ」と、時間に対応した「滞在場所」と、同様に時間に対応した「発信元電話番号であるアクセス権」とから構成されている。

【００１７】つぎに、この実施の形態１に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図３及び図５は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図４は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【００１８】ユーザは、図２に示すように、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザＩＤ」と、一日の時間に対応した「滞在場所」及び「アクセ

ス権（発信元電話番号)」をスケジュール管理装置７を介してファイル装置８に登録しておく。スケジュールテーブルで、アクセス権を「禁止」にした時間中は、公衆網２からのアクセスを禁止する。一方、スケジュールテーブルのアクセス権に「電話番号」を登録すると、その電話番号からの発信についてのみ公衆網２からのアクセスを許可する。

【００１９】上述したように、ユーザは、予めスケジュール管理ツールに行動スケジュールを登録しておく。そして、アクセスサーバ３Ａは、公衆網２からの接続要求を受けたとき、携帯端末１で使用している電話番号（発信元電話番号）を公衆網２から受けとる。この時、「ユーザＩＤ」と「発信元電話番号」をスケジュール管理ツールへ渡す。

【００２０】スケジュール管理ツールでは、受けた「ユーザＩＤ」に対応した行動スケジュールを検索し、当該電話番号からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ３Ａへ結果を返す。

【００２１】アクセスサーバ３Ａは、スケジュール管理ツールの判定結果が「認可」であれば、携帯端末１と組織内ネットワーク間の接続（通信）を、携帯端末１からの切断要求を受けるまで保持し、判定結果が「否認」であれば、直ちに通信を切断する。

【００２２】すなわち、図３のステップ１０において、アクセスサーバ３Ａは、携帯端末１からアクセス要求を受け付ける。

【００２３】次に、ステップ１１において、アクセスサーバ３Ａは、携帯端末１から、「ユーザＩＤ」と、「パスワード」と、「発信元電話番号」を受け取る。

【００２４】次に、ステップ１２において、受け取った「ユーザＩＤ」及び「パスワード」を、ファイル装置６に登録されているユーザＩＤ及びパスワードと比較する。

【００２５】次に、ステップ１３～１４において、携帯端末１から受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ３Ａは「ユーザＩＤ」及び「発信元電話番号」をスケジュール管理装置７に送る。

【００２６】ステップ１５～１６において、アクセスサーバ３Ａは、携帯端末１から受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末１に通知し、携帯端末１との接続を断つ。

【００２７】つづいて、図４のステップ２０において、スケジュール管理装置７は、「ユーザＩＤ」及び「発信元電話番号」をアクセスサーバ３Ａから受け取る。

【００２８】次に、ステップ２１～２２において、スケジュール管理装置７は、組織内ネットワーク内の時計から日時を読み込み、「ユーザＩＤ」と現在の時間に基づきファイル装置８内のスケジュールテーブルを検索し、登録された発信元電話番号を読み出す。

【００２９】次に、ステップ２３において、アクセスサーバ３Ａから受け取った「発信元電話番号」を、ファイル装置８から読み出した発信元電話番号と比較する。

【００３０】次に、ステップ２４～２５において、アクセスサーバ３Ａから受け取った「発信元電話番号」と登録内容が一致した場合は、スケジュール管理装置７はアクセス認可をアクセスサーバ３Ａに通知する。

【００３１】ステップ２６において、スケジュール管理装置７は、アクセスサーバ３Ａから受け取った「発信元電話番号」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ３Ａに通知する。
【００３２】つづいて、図５のステップ３０において、アクセスサーバ３Ａは、アクセス可否判定結果をスケジュール管理装置７から受け取る。
【００３３】次に、ステップ３１～３３において、スケジュール管理装置７からアクセス認可を受け取った場合は、アクセスサーバ３Ａはアクセス許可を携帯端末１に通知し、組織内ネットワークとの通信を許可する。
【００３４】ステップ３４～３５において、アクセスサーバ３Ａは、スケジュール管理装置７からアクセス否認を受け取った場合には、アクセス拒否を携帯端末１に通知し、携帯端末１との接続を断つ。
【００３５】この実施の形態１に係る不正アクセス防止システムは、組織外にある端末１から公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７とアクセスサーバ３Ａを連携させ、ユーザＩＤ及びパスワードと、携帯端末１Ａの電話番号とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。
【００３６】実施の形態２．この発明の実施の形態２に係る不正アクセス防止システムについて図面を参照しながら説明する。上記の実施の形態１ではスケジュール管理装置７で発信元電話番号を登録内容と比較しアクセス可否を判定していたが、この実施の形態２ではアクセスサーバ３Ｂがアクセス可否の判定を行う。
【００３７】なお、この実施の形態２に係る不正アクセス防止システムの構成は、上記の実施の形態１とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を３Ｂ及び７Ａとする。
【００３８】図６及び図８は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図７は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。
【００３９】図６のステップ４０において、アクセスサーバ３Ｂは、携帯端末１からアクセス要求を受け付ける。
【００４０】次に、ステップ４１において、アクセスサーバ３Ｂは、携帯端末１から、「ユーザＩＤ」と、「パスワード」と、「発信元電話番号」を受け取る。
【００４１】次に、ステップ４２において、受け取った「ユーザＩＤ」及び「パスワード」を、ファイル装置６に登録されているユーザＩＤ及びパスワードと比較する。
【００４２】次に、ステップ４３～４４において、携帯端末１から受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ３Ｂは「ユーザＩＤ」をスケジュール管理装置７Ａに送る。
【００４３】ステップ４５～４６において、アクセスサーバ３Ｂは、携帯端末１から受け

取った「ユーザＩＤ」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末１に通知し、携帯端末１との接続を断つ。

【００４４】つづいて、図７のステップ５０において、スケジュール管理装置７Ａは、「ユーザＩＤ」をアクセスサーバ３Ｂから受け取る。

【００４５】次に、ステップ５１～５２において、スケジュール管理装置７Ａは、組織内ネットワーク内の時計から日時を読み込み、「ユーザＩＤ」と現在の時間に基づきファイル装置８内のスケジュールテーブルを検索し、登録された発信元電話番号等のアクセス権データを読み出す。

【００４６】次に、ステップ５３において、スケジュール管理装置７Ａは、読み出したアクセス権データをアクセスサーバ３Ｂに通知する。

【００４７】つづいて、図８のステップ６０において、アクセスサーバ３Ｂは、アクセス権データをスケジュール管理装置７Ａから受け取る。

【００４８】次に、ステップ６１において、アクセスサーバ３Ｂは、携帯端末１から受け取った「発信元電話番号」とアクセス権データの内容である発信元電話番号が一致した場合は、アクセス認可と判定する。一方、携帯端末１から受け取った「発信元電話番号」とアクセス権データの内容である発信元電話番号が一致しなかった場合には、アクセス否認と判定する。さらに、アクセスサーバ３Ｂは、アクセス権データの内容が禁止である場合はアクセス否認と判定する。

【００４９】次に、ステップ６２～６４において、アクセス認可と判定した場合は、アクセスサーバ３Ｂはアクセス許可を携帯端末１に通知し、組織内ネットワークとの通信を許可する。

【００５０】ステップ６５～６６において、アクセスサーバ３Ｂは、アクセス否認と判定した場合には、アクセス拒否を携帯端末１に通知し、携帯端末１との接続を断つ。

【００５１】この実施の形態２に係る不正アクセス防止システムは、組織外にある端末１から公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７Ａとアクセスサーバ３Ｂを連携させ、ユーザＩＤ及びパスワードと、携帯端末１の電話番号とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【００５２】実施の形態３．この発明の実施の形態３に係る不正アクセス防止システムについて図面を参照しながら説明する。図９は、この発明の実施の形態３に係る不正アクセス防止システムの構成を示す図である。

【００５３】図９において、１ＡはＧＰＳ機能を有する携帯端末、２は公衆網、３Ｃは組織内ネットワークのアクセスサーバ、４は組織内ネットワークのクライアント、６はユーザ毎のユーザＩＤとパスワードが登録されているファイル装置、７Ｂは組織内ネットワークのスケジュール管理装置、８は個人のスケジュールテーブルが登録されているファイル装置である。

【００５４】図１０は、この発明の実施の形態３に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【００５５】図１０に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザ一人について「ユーザ番号」と、「ユーザＩＤ」と、時間に対応した「滞在場所」と、同様に時間に対応した「住所（位置情報）」とから構成されている。

【００５６】つぎに、この実施の形態３に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図１１及び図１３は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図１２は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【００５７】図１０に示すように、ユーザは、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザＩＤ」と、一日の時間に対応した「滞在場所」及び「住所（位置情報）」をスケジュール管理装置７Ｂを介してファイル装置８に登録しておく。

【００５８】上述したように、ユーザは予めスケジュール管理ツールに行動スケジュールを登録しておき、また、ＧＰＳ機能を備えた携帯端末１Ａを持つ。そして、アクセスサーバ３Ｃは、公衆網２からの接続要求を受けた時、ＧＰＳ機能により認識された「位置情報」を受け取り、「ユーザＩＤ」と「位置情報」をスケジュール管理ツールへ渡す。

【００５９】スケジュール管理ツールでは、受けた「ユーザＩＤ」に対応した行動スケジュールを検索し、当該位置情報に対応する地域からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ３Ｃへ判定結果を返す。この場合の位置情報は、誤差が発生する可能性があるので、必要に応じてアクセスを許可する地域に余裕を持たせる。

【００６０】アクセスサーバ３Ｃでは、スケジュール管理ツールの判定結果が認可であれば携帯端末１Ａと組織内ネットワーク間の接続（通信）を、携帯端末１Ａからの切断要求を受けるまで保持し、判定結果が否認であれば直ちに通信を切断する。

【００６１】すなわち、図１１のステップ７０において、アクセスサーバ３Ｃは、携帯端末１Ａからアクセス要求を受け付ける。

【００６２】次に、ステップ７１において、アクセスサーバ３Ｃは、携帯端末１Ａから、「ユーザＩＤ」と、「パスワード」と、「位置情報」を受け取る。

【００６３】次に、ステップ７２において、受け取った「ユーザＩＤ」及び「パスワード」を、ファイル装置６に登録されているユーザＩＤ及びパスワードと比較する。

【００６４】次に、ステップ７３～７４において、携帯端末１Ａから受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ３Ｃは「ユーザＩＤ」及び「位置情報」をスケジュール管理装置７Ｂに送る。

【００６５】ステップ７５～７６において、アクセスサーバ３Ｃは、携帯端末１Ａから受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末１Ａに通知し、携帯端末１Ａとの接続を断つ。

【００６６】つづいて、図１２のステップ８０において、スケジュール管理装置７Ｂは、「ユ

ーザＩＤ」及び「位置情報」をアクセスサーバ３Ｃから受け取る。

【００６７】次に、ステップ８１～８２において、スケジュール管理装置７Ｂは、組織内ネットワーク内の時計から日時を読み込み、「ユーザＩＤ」と現在の時間に基づきファイル装置８内のスケジュールテーブルを検索し、登録された位置情報を読み出す。

【００６８】次に、ステップ８３において、アクセスサーバ３Ｃから受け取った「位置情報」を、ファイル装置８から読み出した位置情報と比較する。

【００６９】次に、ステップ８４～８５において、アクセスサーバ３Ｃから受け取った「位置情報」と登録内容が一致した場合は、スケジュール管理装置７Ｂはアクセス認可をアクセスサーバ３Ｃに通知する。

【００７０】ステップ８６において、スケジュール管理装置７Ｂは、アクセスサーバ３Ｃから受け取った「位置情報」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ３Ｃに通知する。

【００７１】つづいて、図１３のステップ９０において、アクセスサーバ３Ｃは、アクセス可否判定結果をスケジュール管理装置７Ｂから受け取る。

【００７２】次に、ステップ９１～９３において、スケジュール管理装置７Ｂからアクセス認可を受け取った場合は、アクセスサーバ３Ｃはアクセス許可を携帯端末１Ａに通知し、組織内ネットワークとの通信を許可する。

【００７３】ステップ９４～９５において、アクセスサーバ３Ｃは、スケジュール管理装置７Ｂからアクセス否認を受け取った場合には、アクセス拒否を携帯端末１Ａに通知し、携帯端末１Ａとの接続を断つ。

【００７４】この実施の形態３に係る不正アクセス防止システムは、組織外にある端末１Ａから公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７Ｂとアクセスサーバ３Ｃを連携させ、ユーザＩＤ及びパスワードと、携帯端末１Ａの位置情報とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【００７５】実施の形態４．この発明の実施の形態４に係る不正アクセス防止システムについて説明する。上記の実施の形態３ではスケジュール管理装置７Ｂで位置情報を登録内容と比較しアクセス可否を判定していたが、この実施の形態４ではアクセスサーバ３Ｄがアクセス可否の判定を行うものである。

【００７６】なお、この実施の形態４に係る不正アクセス防止システムの構成は、上記の実施の形態３とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を３Ｄ及び７Ｃとする。

【００７７】また、この実施の形態４に係る不正アクセス防止システムの動作は、図６～図８に示す実施の形態２のアクセスサーバ及びスケジュール管理装置の動作と基本的には同様であるので図示を省略する。異なる点は、アクセス権データの代わりに位置情報となるだけである。

【００７８】この実施の形態４に係る不正アクセス防止システムは、組織外にある端末１Ａから公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７Ｃとアクセスサーバ３Ｄを連携させ、ユーザＩＤ及びパスワードと、携帯端末１Ａの位置情報とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【００７９】実施の形態５．この発明の実施の形態５に係る不正アクセス防止システムについて図面を参照しながら説明する。図１４は、この発明の実施の形態５に係る不正アクセス防止システムの構成を示す図である。

【００８０】図１４において、１ＡはＧＰＳ機能を有する携帯端末、２は公衆網、３Ｅは組織内ネットワークのアクセスサーバ、４は組織内ネットワークのクライアント、６はユーザ毎のユーザＩＤとパスワードが登録されているファイル装置、７Ｄは組織内ネットワークのスケジュール管理装置、８は個人のスケジュールテーブルが登録されているファイル装置である。

【００８１】図１５は、この発明の実施の形態５に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【００８２】図１５に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザー人について「ユーザ番号」と、「ユーザＩＤ」と、時間に対応した「滞在場所」と、同様に時間に対応した「住所（位置情報)」と、同様に時間に対応した「アクセス権（発信元電話番号)」とから構成されている。

【００８３】つぎに、この実施の形態５に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図１６及び図１８は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図１７は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【００８４】図１５に示すように、ユーザは、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザＩＤ」と、一日の時間に対応した「滞在場所」、「住所（位置情報)」及び「アクセス権（発信元電話番号)」をスケジュール管理装置７Ｄを介してファイル装置８に登録しておく。スケジュールテーブルで、アクセス権を「禁止」にした時間中は、公衆網２からのアクセスを禁止する。一方、スケジュールテーブルのアクセス権に「電話番号」を登録し、かつスケジュールテーブルの住所（位置情報）に場所を登録すると、その電話番号から、かつ登録した場所からの発信についてのみ公衆網２からのアクセスを許可する。

【００８５】上述したように、ユーザは予めスケジュール管理ツールに行動スケジュールを登録しておき、また、ＧＰＳ機能を備えた携帯端末１Ａを持つ。そして、アクセスサーバ３Ｅは、公衆網２からの接続要求を受けた時、使用している携帯端末１Ａの電話番号（発信元電話番号）を公衆網２から受け取る。さらに、ＧＰＳ機能により認識された「位置情報」を受け取り、「ユーザＩＤ」と「発信元電話番号」と「位置情報」をスケジュール管理

ツールへ渡す。

【００８６】スケジュール管理ツールでは、受けた「ユーザＩＤ」に対応した行動スケジュールを検索し、当該電話番号及び当該位置情報に対応する地域からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ３Ｅへ判定結果を返す。この場合の位置情報は、誤差が発生する可能性があるので、必要に応じてアクセスを許可する地域に余裕を持たせる。

【００８７】アクセスサーバ３Ｅでは、スケジュール管理ツールの判定結果が認可であれば携帯端末１Ａと組織内ネットワーク間の接続（通信）を、携帯端末１Ａからの切断要求を受けるまで保持し、判定結果が否認であれば直ちに通信を切断する。

【００８８】すなわち、図１６のステップ１００において、アクセスサーバ３Ｅは、携帯端末１Ａからアクセス要求を受け付ける。

【００８９】次に、ステップ１０１において、アクセスサーバ３Ｅは、携帯端末１Ａから、「ユーザＩＤ」と、「パスワード」と、「発信元電話番号」と、「位置情報」を受け取る。

【００９０】次に、ステップ１０２において、受け取った「ユーザＩＤ」及び「パスワード」を、ファイル装置６に登録されているユーザＩＤ及びパスワードと比較する。

【００９１】次に、ステップ１０３～１０４において、携帯端末１Ａから受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ３Ｅは「ユーザＩＤ」、「発信元電話番号」及び「位置情報」をスケジュール管理装置７Ｂに送る。

【００９２】ステップ１０５～１０６において、アクセスサーバ３Ｅは、携帯端末１Ａから受け取った「ユーザＩＤ」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末１Ａに通知し、携帯端末１Ａとの接続を断つ。

【００９３】つづいて、図１７のステップ１１０において、スケジュール管理装置７Ｄは、「ユーザＩＤ」、「発信元電話番号」及び「位置情報」をアクセスサーバ３Ｃから受け取る。

【００９４】次に、ステップ１１１～１１２において、スケジュール管理装置７Ｄは、組織内ネットワーク内の時計から日時を読み込み、「ユーザＩＤ」と現在の時間に基づきファイル装置８内のスケジュールテーブルを検索し、登録された発信元電話番号及び位置情報を読み出す。

【００９５】次に、ステップ１１３において、アクセスサーバ３Ｅから受け取った「発信元電話番号」及び「位置情報」を、ファイル装置８から読み出した発信元電話番号及び位置情報と比較する。

【００９６】次に、ステップ１１４～１１５において、アクセスサーバ３Ｅから受け取った「発信元電話番号」及び「位置情報」と登録内容が一致した場合は、スケジュール管理装置７Ｄはアクセス認可をアクセスサーバ３Ｅに通知する。

【００９７】ステップ１１６において、スケジュール管理装置７Ｄは、アクセスサーバ３Ｅから受け取った「発信元電話番号」及び「位置情報」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ３Ｅに通知する。

【００９８】つづいて、図１８のステップ１２０において、アクセスサーバ３Ｅは、アクセス可否判定結果をスケジュール管理装置７Ｄから受け取る。
【００９９】次に、ステップ１２１～１２３において、スケジュール管理装置７Ｄからアクセス認可を受け取った場合は、アクセスサーバ３Ｅはアクセス許可を携帯端末１Ａに通知し、組織内ネットワークとの通信を許可する。
【０１００】ステップ１２４～１２５において、アクセスサーバ３Ｅは、スケジュール管理装置７Ｄからアクセス否認を受け取った場合には、アクセス拒否を携帯端末１Ａに通知し、携帯端末１Ａとの接続を断つ。
【０１０１】この実施の形態５に係る不正アクセス防止システムは、組織外にある端末１Ａから公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７Ｄとアクセスサーバ３Ｅを連携させ、ユーザＩＤ及びパスワードと、携帯端末１Ａの電話番号及び位置情報とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。
【０１０２】実施の形態６．この発明の実施の形態６に係る不正アクセス防止システムについて説明する。上記の実施の形態５ではスケジュール管理装置７Ｄで発信元電話番号及び位置情報を登録内容と比較しアクセス可否を判定していたが、この実施の形態６ではアクセスサーバ３Ｆがアクセス可否の判定を行うものである。
【０１０３】なお、この実施の形態６に係る不正アクセス防止システムの構成は、上記の実施の形態５とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を３Ｆ及び７Ｅとする。
【０１０４】また、この実施の形態６に係る不正アクセス防止システムの動作は、図６～図８に示す実施の形態２のアクセスサーバ及びスケジュール管理装置の動作と基本的には同様であるので図示を省略する。異なる点は、アクセス権データに位置情報が加えられているだけである。
【０１０５】この実施の形態６に係る不正アクセス防止システムは、組織外にある端末１Ａから公衆網２経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置７Ｅとアクセスサーバ３Ｆを連携させ、ユーザＩＤ及びパスワードと、携帯端末１Ａの電話番号及び位置情報とに基づき２重に接続可否を判定することにより、セキュリティの強化を図ることができる。
【０１０６】
【発明の効果】この発明に係る不正アクセス防止システムは、以上説明したとおり、携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤ及び第１のユーザ識別情報を受け取り前記第１のユーザ識別情報とスケジュールテーブルに予め登録された

第２のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤ及び第１のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第１及び第２のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知するので、２重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【０１０７】この発明に係る不正アクセス防止システムは、以上説明したとおり、携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザＩＤを受け取り前記ユーザＩＤに基づきスケジュールテーブルから予め登録された第２のユーザ識別情報を読み出して前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザＩＤ、パスワード及び第１のユーザ識別情報を受け取り前記ユーザＩＤ及びパスワードと登録内容と比較して一致したときは前記ユーザＩＤを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第２のユーザ識別情報を受け取り前記第１及び第２のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するので、２重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【０１０８】また、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第１及び第２のユーザ識別情報を、前記携帯端末の発信元電話番号としたので、２重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【０１０９】また、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第１のユーザ識別情報を、前記携帯端末の位置情報とし、前記第２のユーザ識別情報を、前記登録された位置情報としたので、２重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【０１１０】さらに、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第１のユーザ識別情報を、前記携帯端末の発信元電話番号及び位置情報とし、前記第２のユーザ識別情報を、前記携帯端末の発信元電話番号及び前記登録された位置情報としたので、２重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

図の説明

【図面の簡単な説明】

【図１】 この発明の実施の形態１に係る不正アクセス防止システムの構成を示す図である。

【図２】 この発明の実施の形態１に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図３】 この発明の実施の形態１に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図４】 この発明の実施の形態１に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図５】 この発明の実施の形態１に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図６】 この発明の実施の形態２に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図７】 この発明の実施の形態２に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図８】 この発明の実施の形態２に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図９】 この発明の実施の形態３に係る不正アクセス防止システムの構成を示す図である。

【図１０】 この発明の実施の形態３に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図１１】 この発明の実施の形態３に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図１２】 この発明の実施の形態３に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図１３】 この発明の実施の形態３に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図１４】 この発明の実施の形態５に係る不正アクセス防止システムの構成を示す図である。

【図１５】 この発明の実施の形態５に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図１６】 この発明の実施の形態５に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図１７】 この発明の実施の形態５に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図１８】 この発明の実施の形態５に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

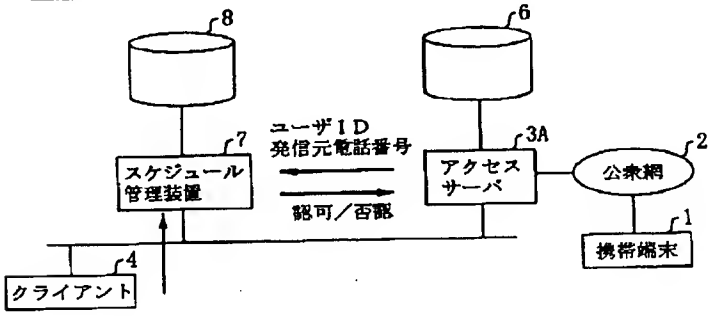
【図１９】 従来の不正アクセス防止システムの構成を示す図である。

【符号の説明】

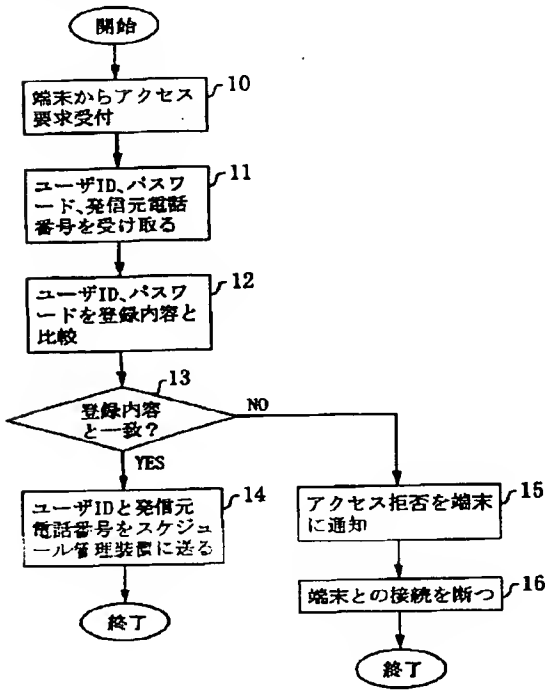
１ 携帯端末、１Ａ ＧＰＳ機能を備えた携帯端末、２ 公衆網、３Ａ、３Ｂ、３Ｃ、３Ｄ、３Ｅ、３Ｆ アクセスサーバ、４ クライアント、６ ファイル装置、７、７Ａ、７Ｂ、７Ｃ、７Ｄ、７Ｅ スケジュール管理装置、８ ファイル装置。

図面

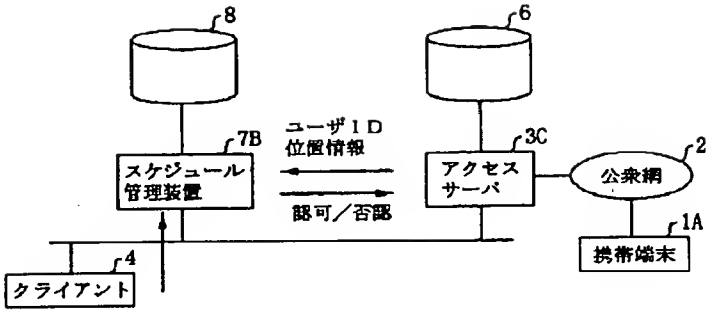
【図１】



【図３】



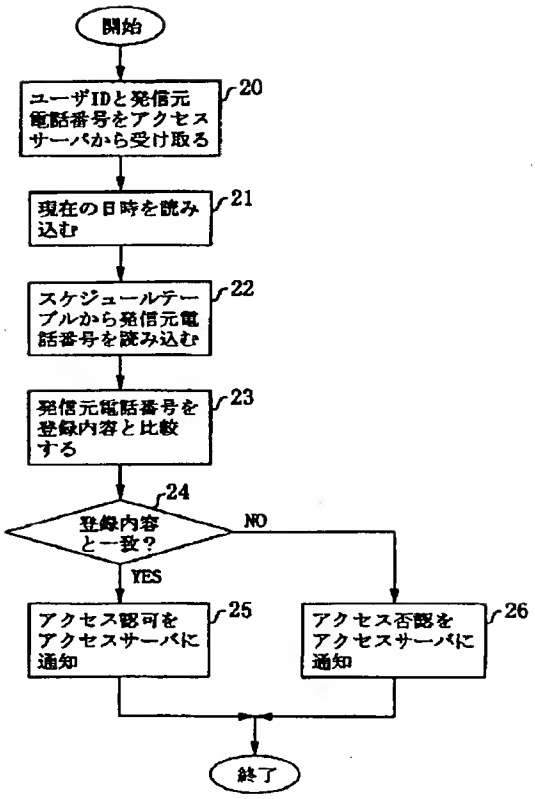
【図９】



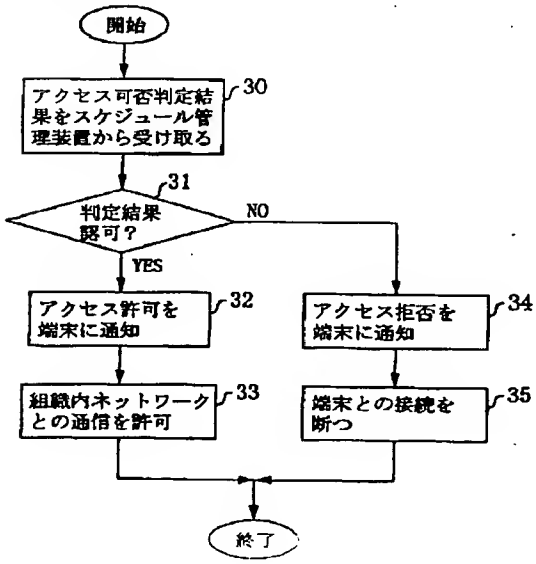
【図２】

ユーザ番号	ユーザＩＤ	時間	・・・9	10	11	12	13	14	15	16	17	18	19	20・・・
1	user1	滞在場所	～	構内				移動	X大学			移動	自宅	
		アクセス権（発信元電話番号）	～	禁止				030-XX-XXXXX	030-XX-XXXXX			030-XX-XXXXX	030-XX-XXXXX	
2	user2	滞在場所	～	構内	移動	Y社		移動	Z事業所			移動	自宅	
		アクセス権（発信元電話番号）	～	禁止	030-XX-XXXXX	030-XX-XXXXX		030-XX-XXXXX	030-XX-XXXXX			030-XX-XXXXX	045-XXX-XXXX	
3	user3	滞在場所	自宅											
		アクセス権（発信元電話番号）	03-XXXX-XXXX											
～	～	～	～											

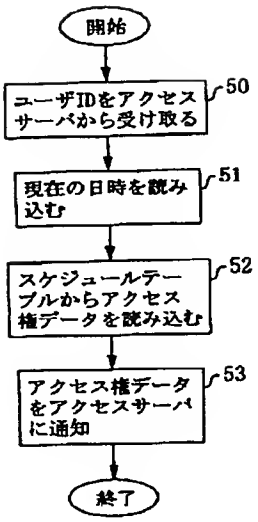
【図４】


開始
ユーザIDと発信元電話番号をアクセスサーバから受け取る
20
現在の日時を読み込む
21
スケジュールテーブルから発信元電話番号を読み込む
22
発信元電話番号を登録内容と比較する
23
登録内容と一致？
24
NO
YES
アクセス認可をアクセスサーバに通知
25
アクセス否認をアクセスサーバに通知
26
終了

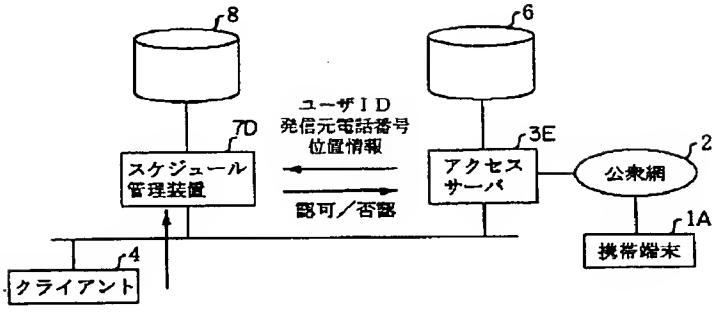
【図５】


開始
アクセス可否判定結果をスケジュール管理装置から受け取る
30
判定結果認可？
31
NO
YES
アクセス許可を端末に通知
32
アクセス拒否を端末に通知
34
組織内ネットワークとの通信を許可
33
端末との接続を断つ
35
終了

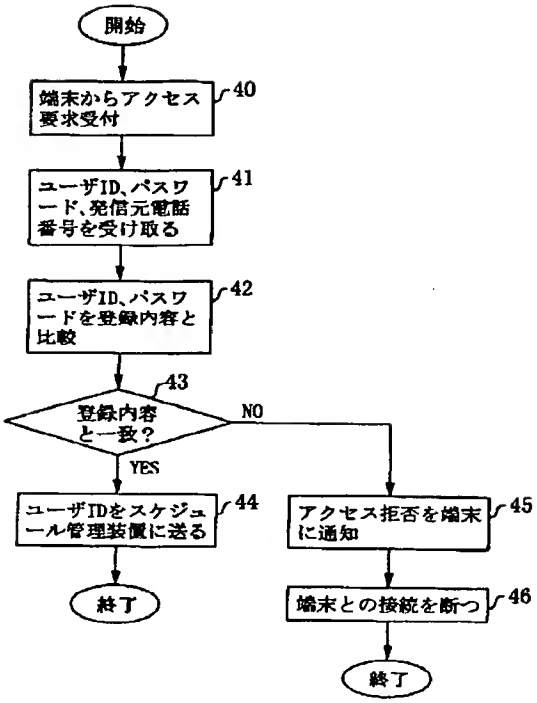
【図７】


開始
ユーザIDをアクセスサーバから受け取る
50
現在の日時を読み込む
51
スケジュールテーブルからアクセス権データを読み込む
52
アクセス権データをアクセスサーバに通知
53
終了

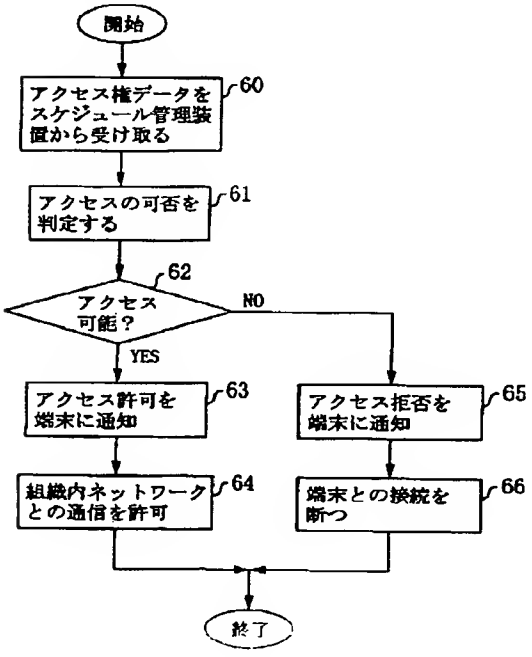
【図１４】


8
6
ユーザＩＤ
発信元電話番号
位置情報
7D
3E
2
スケジュール管理装置
アクセスサーバ
公衆網
許可／否認
1A
4
クライアント
携帯端末

【図６】


開始
端末からアクセス要求受付
40
ユーザID、パスワード、発信元電話番号を受け取る
41
ユーザID、パスワードを登録内容と比較
42
43
登録内容と一致？
NO
YES
ユーザIDをスケジュール管理装置に送る
44
アクセス拒否を端末に通知
45
終了
端末との接続を断つ
46
終了

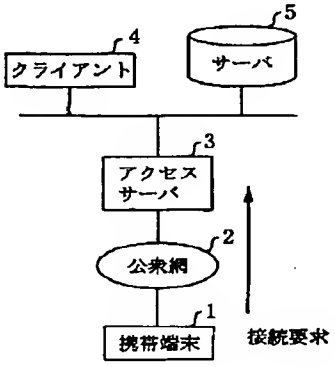
【図８】


開始
アクセス権データをスケジュール管理装置から受け取る
60
アクセスの可否を判定する
61
62
アクセス可能？
NO
YES
アクセス許可を端末に通知
63
アクセス拒否を端末に通知
65
組織内ネットワークとの通信を許可
64
端末との接続を断つ
66
終了

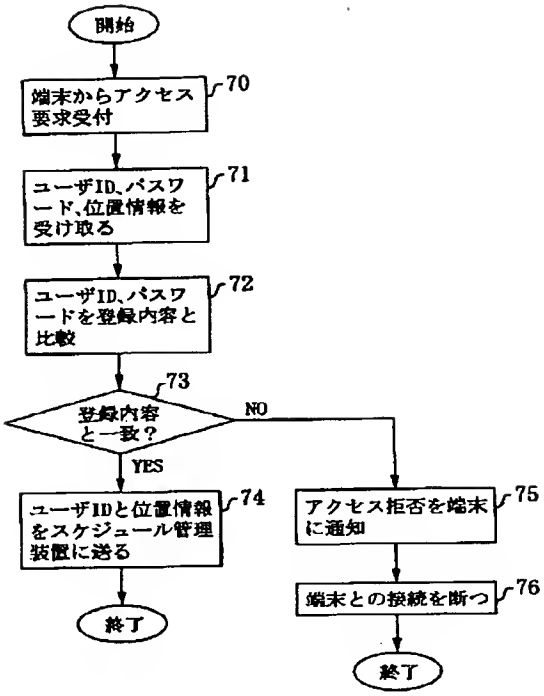
【図１０】

ユーザ番号	ユーザID	時間	・・・9	10	11	12	13	14	15	16	17	18	19	20・・・
1	user1	滞在場所	～	構内				移動	X大学			移動		自宅
		住所(位置情報)	～	A市K区				A市、B市	B市L町			B市、C市		C市M区
2	user2	滞在場所	～	構内		移動	Y社		移動	Z事業所		移動		自宅
		住所(位置情報)	～	A市K区		A市、D市	D市N町		D市	D市O町		D市、E市		E市P町
3	user3	滞在場所	自宅											
		住所(位置情報)	A市Q区											
≀	≀	≀	≀											

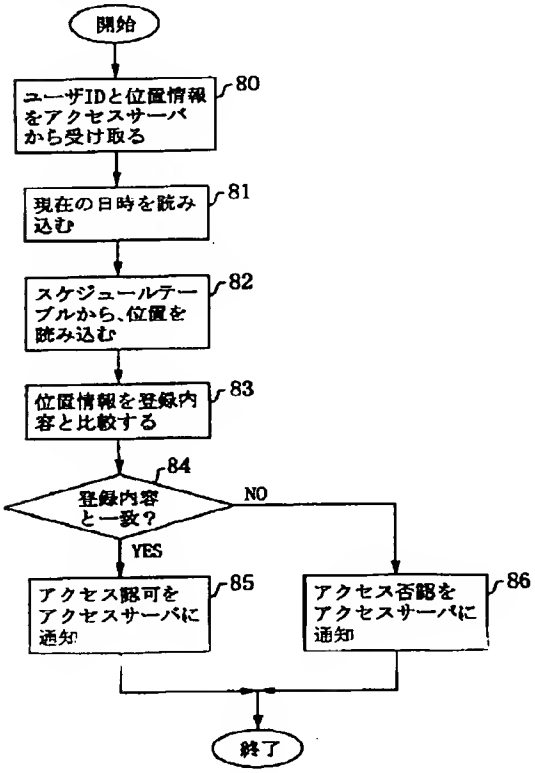
【図１９】



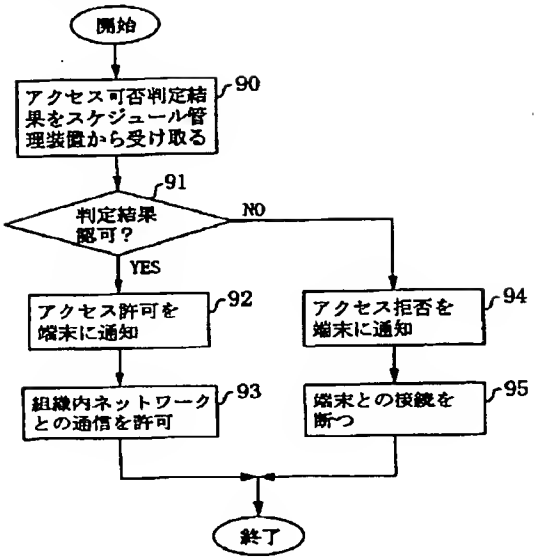
【図１１】


開始
端末からアクセス要求受付
70
ユーザID、パスワード、位置情報を受け取る
71
ユーザID、パスワードを登録内容と比較
72
73
登録内容と一致？
NO
YES
ユーザIDと位置情報をスケジュール管理装置に送る
74
アクセス拒否を端末に通知
75
端末との接続を断つ
76
終了
終了

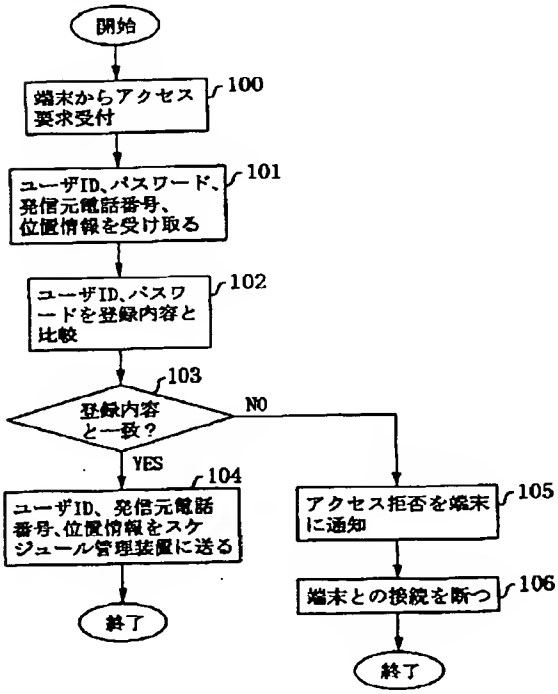
【図１２】


開始
ユーザIDと位置情報をアクセスサーバから受け取る
80
現在の日時を読み込む
81
スケジュールテーブルから、位置を読み込む
82
位置情報を登録内容と比較する
83
84
登録内容と一致？
NO
YES
アクセス認可をアクセスサーバに通知
85
アクセス否認をアクセスサーバに通知
86
終了

【図１３】


開始
アクセス可否判定結果をスケジュール管理装置から受け取る
90
判定結果認可？
91
NO
YES
アクセス許可を端末に通知
92
アクセス拒否を端末に通知
94
組織内ネットワークとの通信を許可
93
端末との接続を断つ
95
終了

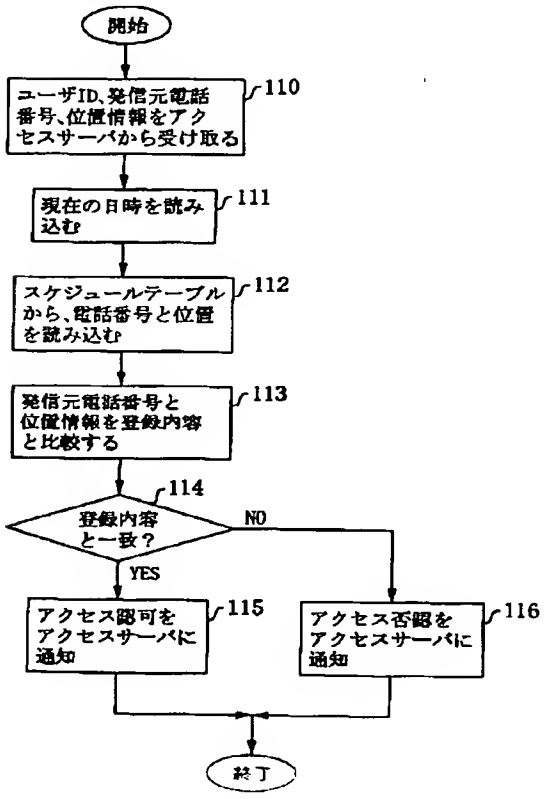
【図１６】


開始
端末からアクセス要求受付
100
ユーザID、パスワード、発信元電話番号、位置情報を受け取る
101
ユーザID、パスワードを登録内容と比較
102
登録内容と一致？
103
NO
YES
ユーザID、発信元電話番号、位置情報をスケジュール管理装置に送る
104
アクセス拒否を端末に通知
105
端末との接続を断つ
106
終了
終了

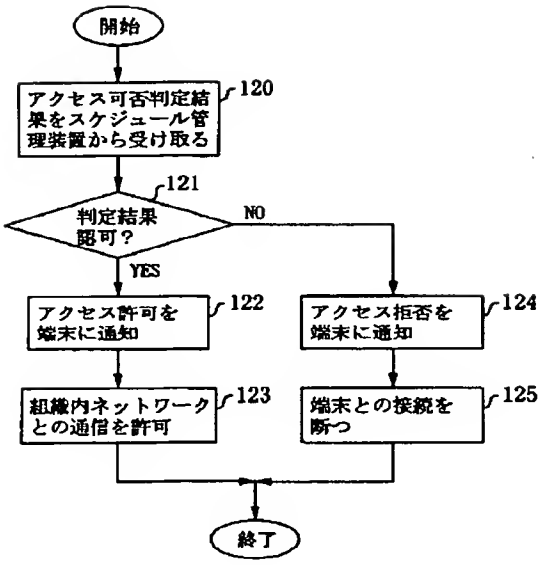
【図１５】

ユーザ番号	ユーザID	時間	・・・9	10	11	12	13	14	15	16	17	18	19	20	・・・
1	user1	滞在場所	～	構内			移動			X大学			移動		自宅
		住所（位置情報）	～	A市K区			A市、B市			B市L町			B市、C市		C市M区
		アクセス権（発信元電話番号）	～	禁止			030-XX-XXXX			030-XX-XXXX			030-XX-XXXX		030-XX-XXXX
2	user2	滞在場所	～	構内		移動		Y社		移動		Z事業所	移動		自宅
		住所（位置情報）	～	A市K区		A市、D市		D市N町		D市		D市O町	D市、E市		E市P町
		アクセス権（発信元電話番号）	～	禁止		030-XX-XXXX		030-XX-XXXX		030-XX-XXXX		030-XX-XXXX	030-XX-XXXX		045-XXX-XXXX
3	user3	滞在場所	自宅												
		住所（位置情報）	A市Q区												
		アクセス権（発信元電話番号）	03-XXXX-XXXX												
｜	｜	｜	｜												

【図１７】



【図１８】


開始
アクセス可否判定結果をスケジュール管理装置から受け取る
120
121
判定結果認可？
NO
YES
アクセス許可を端末に通知
122
アクセス拒否を端末に通知
124
組織内ネットワークとの通信を許可
123
端末との接続を断つ
125
終了